Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 09 March 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports the Department of Treasury is setting up a new office, called the Office of Terrorism and Financial Intelligence, to coordinate efforts to stop the flow of money to terrorists. (See item 5)
- The Age reports the Australian Federal Government is set to toughen access to ammonium nitrate, the common fertilizer used by terrorists to make simple, but powerful bombs. (See item 20)
- Techworld.com reports HP Tru64 Unix, Hewlett−Packard Co.'s OS, has been found to suffer from "highly critical" security flaws involving remote access to systems. (See item 24)
- Security Focus has raised ThreatCon to Level 2, requiring increased vigilance. Please refer to the Internet Alert Dashboard.

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *March 08, Reuters* — **Thousands still without power in Carolinas. Utilities in the Carolinas said Monday, March 8, wind and thunderstorms knocked out power to nearly 400,000 electric customers late Sunday, March 7. There were still about 130,000 homes and**

businesses without electric service at noon Monday. The storm's wind and rain weighed down trees and branches, dropping them onto power lines. The hardest hit utilities were owned by Duke Energy Corp., which lost about 206,000 customers at the height of the storm. At about 8 a.m., Duke, which serves about 2.1 million customers in North and South Carolina, said it had about 113,000 customers still without service. Duke spokesperson Tom Williams said the company was not able to project how long it would take to restore power to all customers.
Source: http://biz.yahoo.com/rm/040308/utilities_duke_outages_1.html

2. *March 08, Nuclear Regulatory Commission* — **NRC approves Davis−Besse restart. The Nuclear Regulatory Commission (NRC) staff has approved the restart of the Davis−Besse Nuclear Power Plant, which has been shut down since February 2002 for replacement of a damaged reactor vessel head and other safety improvements.** The plant near Oak Harbor, OH, is operated by FirstEnergy Nuclear Operating Company. James Caldwell, Regional Administrator for the agency's Region III office in Lisle, IL, approved restart of the plant in a letter to the utility issued Monday, March 8, subject to the utility's compliance with its license requirements and NRC regulations. **During the startup, the NRC will maintain round the clock inspection coverage of plant activities.** Expanded inspection coverage at Davis−Besse will continue beyond startup. There are three resident inspectors assigned to Davis−Besse, one more than the normal staffing. With its restart decision, the NRC issued a Confirmatory Order to FirstEnergy requiring independent assessments and inspections at the Davis−Besse Nuclear Power Station to provide reasonable assurance that the long−term corrective actions remain effective.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2004/04−0 11iii.html

[Return to top]

Chemical Sector

3. *March 08, Click2Houston* — **Gas leaks from Texas chemical plant. Deer Park, TX, officials issued a level three shelter−in−place warning Monday morning, March 8, after a gas leak was discovered at the Dow Chemical Plant, News2Houston reported. Traces of the chemical napthalene, which is used to make mothballs, were discovered outside the plant's boundaries around 6:15 a.m.** The city of Deer Park was notified and officials issued the level three warning, alerting people to stay indoors, keeping doors and windows closed, until further notice. Officials are not sure what caused the chemical leak. Dow Chemical Plant officials are working to get the situation under control.
Source: http://www.click2houston.com/news/2904249/detail.html

[Return to top]

Defense Industrial Base Sector

4. *March 06, Copley News Service* — **Army, Marines await updates of combat rifles.** Most of the Marines going into Iraq will carry a new model of the M−16 rifle, beginning a process that will give virtually all Marines an improved personal weapon over the next several years. The M−16 has been the standard personal weapon for the U.S. military for more than 40 years. **The**

new M−16A4 will facilitate attachment of a variety of high−tech sights and other devices to improve troops' ability to fight in varying conditions. However, while the Marines are sticking with the familiar U.S.−designed M−16, the Army is expected to adopt a radically different rifle developed by the German firm Heckler and Koch. That would mean that soldiers and Marines would have different combat rifles for the first time in a century. **The Army's rifle is in the final testing stage and will integrate a high−tech sight. The rifle, currently designated the XM8, is a spinoff of a long−range Army program to develop the "objective individual weapon."** It is intended to combine an 5.56mm rifle with a weapon that uses laser−range finding to explode a 20mm projectile over a concealed enemy.
Source: http://www.signonsandiego.com/news/military/20040306−9999−ne ws_1n6rifles.html

[Return to top]

Banking and Finance Sector

5. *March 08, Associated Press* — **Feds seek to block money to terrorists. The Department of Treasury is setting up a new office, called the Office of Terrorism and Financial Intelligence, to coordinate efforts to stop the flow of money to terrorists.** "The new office will not only focus on the financial war on terror, but protect the integrity of the financial system, fight financial crime, enforce economic sanctions against rogue nations and assist in the ongoing hunt for Iraqi assets," a department statement said Monday, March 8. **The units now at Treasury that are largely responsible for these various duties −− including the Office of Foreign Assets Control and the Financial Crimes Enforcement Network −− will be part of the new office.** The new office is being set up as the result of a congressional directive signed into law by President Bush late last year. An undersecretary, who would be nominated by the president and subject to Senate confirmation, would be in charge of the new office. The new office "will enhance the precision of our relentless fight to dismantle the terrorists' network of financial and logistical support," said Treasury Secretary John Snow.
Source: http://www.washingtonpost.com/wp−dyn/articles/A39845−2004Mar 8.html

6. *March 07, Xinhuanet* — **China to intensify efforts against money laundering. China's State Administration of Foreign Exchange (SAFE) is planning to launch a computer system to collect information about trading of foreign exchange in large sums of money to further its efforts to fight against money laundering,** SAFE Director Guo Shuqing said Sunday, March 7. **Between March and October last year, the SAFE received information about 2.02 million foreign exchange deals in large sums of money or questionable transactions, involving a total of US$49 million, from designated foreign exchange banks across the country.** "The information helped us uncover and crack down on some 'underground money houses' and cases of illegal foreign exchange trading," said Guo, who is also deputy governor of the People's Bank of China, the country's central bank. The information also provided clues to major cases threatening the nation's financial security, he added. In the first 11 months last year, 338 persons were detained on charges of engaging in the business of "underground money houses" and illegal foreign exchange trading, with US$1.07 million in funds seized, 666 bank accounts with a total of US$8.15 million frozen, and US$2.68 million in fines collected, said Guo.
Source: http://news.xinhuanet.com/english/2004−03/07/content_1350125 .htm

7. *March 06, The News Tribune (WA)* — **Fingerprints could join fight against identity theft. The Washington State House and Senate have approved bills that would let drivers submit a fingerprint to the state Department of Licensing to help protect against identity theft.** However, the measures are different and must be reconciled before legislators send a single bill to Governor Gary Locke. **According to the bills, drivers could voluntarily submit a fingerprint that would be scanned and kept in an agency database, then used to verify a driver's identity when he or she wanted to renew or replace a license.** Supporters want to make it harder for someone to pose as someone else, obtain a license in that person's name, then use it as a gateway to open checking accounts, withdraw money and steal identities. "The reason the banks care is that driver's license is the single most heavily used personal identifier used by financial institutions in Washington state," said Denny Eliason, lobbyist for the Washington Bankers Association. "People use it to cash checks, to withdraw funds, to originate accounts. The more secure we can make that document, the better," he said. Identity theft is a $150 million−a−year problem in Washington, Eliason said.
Source: http://www.tribnet.com/news/local/story/4819917p−4759648c.ht ml

[Return to top]

Transportation Sector

8. *March 08, General Accounting Office* — **GAO−04−94: Intercity Passenger Rail: Amtrak's Management of Northeast Corridor Improvements Demonstrates Need for Best Practices (Report).** Amtrak has not yet met the three−hour trip−time goal established by the 1992 Amtrak Authorization and Development Act, although electrified service between Boston and New York City was initiated in January 2000 and Amtrak began limited high−speed rail service in December 2000. Furthermore, 51 of 72 work elements that FRA identified in its 1994 master plan as necessary to reduce trip times (e.g., electrify tracks and acquire high−speed trains), enhance capacity (e.g., construct sidings), rebuild or extend the life of physical assets (e.g., replace bridges), or make other improvements are incomplete or their status is unknown. **GAO recommends that Amtrak apply best practices for managing large−scale infrastructure projects to future major intercity passenger rail projects and that FRA require these best practices and develop guidance for how to do this.** GAO also recommends that FRA seek legislative authority to oversee such projects in the future. Amtrak did not comment directly on GAO's specific recommendations but said it was incorporating many of the best practices discussed in the report as part of its management restructuring. Highlights: http://www.gao.gov/highlights/d0494high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−94

9. *March 08, Associated Press* — **Zimbabwe seizes U.S. cargo plane, accuses mercenaries. Zimbabwean authorities have seized a U.S.−registered cargo plane carrying 64 "suspected mercenaries" and military equipment, the Home Affairs minister said Monday, March 8.** The Boeing 727−100 was detained at Harare's main airport late Sunday after its owners allegedly made "a false declaration of its cargo and crew," Home Affairs Minister Kembo Mahadi said at a briefing. "The plane was actually carrying 64 suspected mercenaries of various nationalities," he said. "Further investigations also revealed that on board was military material." Mohadi said more details would be released once officials have established "the true identities of the men and their ultimate mission." The plane was moved to a nearby military

base for further investigation, he said. Journalists were not shown the plane and the government's claims could not be independently verified. U.S. Embassy officials said they had not been informed of the incident and were trying to obtain details from Zimbabwe authorities. President Robert Mugabe repeatedly has accused the United States and Britain of plotting to overthrow him.
Source: http://www.usatoday.com/news/world/2004−03−08−zimbabwe_x.htm

[Return to top]

Postal and Shipping Sector

10. *March 08, DM News* — **Prep work prevents mistaken identity for white powder sampler. Direct mail sampling campaigns by a cleaning supply company, which produces a white powder laundry cleaner, have moved smoothly through the mail stream − unlike some similar substances − thanks to advance notice and communication among the U.S. Postal Service, its workers, and the company.** "We make sure we are really upfront with the Postal Service," said Kierie Courtney, direct operations manager of the detergent company. "Because of the nature of sending cleaning products through the mail, we would never want there to be any surprise in the Postal Service about what we are sending." As part of all its sampling campaigns, "through our fulfillment quality process, we put together an actual production prototype of what we are actually going to be sending," she said, "and we physically take that to the post office for confirmation and to get their approval on what we are going to be mailing."
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2674 5

[Return to top]

Agriculture Sector

11. *March 08, Agricultural Research Service* — **Test to find pest−fighting bacteria. A genetic fingerprinting technique developed by Agricultural Research Service (ARS) scientists could point the way to new strains of Pasteuria bacteria with potential to biologically control soybean cyst nematodes.** ARS nematologist Greg Noel and colleagues developed the method to help resolve confusion surrounding Pasteuria's taxonomic classification and clarify its parasite−host relationship with soil−dwelling roundworms like the soybean cyst nematode, a crop pest that costs $324 million to $1.4 billion annually in U.S. soy losses.
Source: http://www.sciencedaily.com/releases/2004/03/040308073847.ht m

12. *March 08, Minnesota Ag Connection* — **No CWD found in Minnesota. Tests on roughly 10,000 deer killed by hunters, in Minnesota, last fall have turned up no signs of chronic wasting disease (CWD), the state Department of Natural Resources (DNR) reported.** No wild deer in Minnesota has tested positive for the fatal brain disease. **So far, deer have been tested in over half of the state's permit areas.** The DNR hopes to complete testing in the remaining sampling areas next fall. CWD is a fatal disease that attacks the brain tissues in deer and elk. Since 2001, the DNR has tested nearly 15,000 wild deer for the disease. CWD was detected in two elk on Minnesota farms in Aitkin and Stearns counties in 2002 and 2003, respectively.

Source: http://www.minnesotaagconnection.com/story−state.cfm?Id=221& yr=2004

13. *March 08, Associated Press* — **Thailand says it's free of bird flu. Thailand declared itself free of bird flu March 8 and announced that farmers will resume breeding chickens next month. No areas of Thailand have had active cases of bird flu in poultry since February 25, more than a month since the country's first case was reported,** said Yukol Limlamthong, director−general of the ministry's Livestock Department of the Agriculture Ministry. Yukol said his office had reported its findings to the World Organization for Animal Health, known as OIE. He said the OIE allows the breeding of new chicken stocks three weeks after no new cases have been found, but the ministry decided to wait until April to ensure there are no new outbreaks. The UN Food and Agriculture Organization and other experts had warned the disease may not be purged from the Asian region for at least a year. **Thailand will continue close observation of previously infected areas until March 17 and an OIE official is expected to inspect breeding areas later this month, Yukol said.** The virus has killed or forced the slaughter of more than 100 million chickens or other fowl in Asia, where outbreaks have been reported in 10 countries and territories.
Source: http://www.sunherald.com/mld/sunherald/news/state/8134547.ht m

14. *March 07, Charlotte Observer* — **Shellfish decline. North Carolina's native oysters are clinging to life. Commercial oyster harvests are down to three percent of their peak a century ago. Development continues to close shellfish beds as streets and parking lots funnel bacteria into once−fertile estuaries. Disease, overfishing, and lost habitat have all hit stocks hard.** "We're probably at the lowest point in recent years, even the past couple of centuries," said Craig Hardy, who heads the North Carolina Division of Marine Fisheries' resource enhancement section. Oysters pump up to 50 gallons of water, pure or putrid, through their gills each day. As they feed on algae, they also filter out sediment and other pollutants. **Robust oysters mean other fish probably are healthy too. Researchers say restoring oyster reefs, which are magnets for hundreds of species, would boost the growth of other seafood.**
Source: http://www.charlotte.com/mld/charlotte/news/8127003.htm

[Return to top]

Food Sector

15. *March 08, Reuters* — **Mexico eases ban on U.S. poultry imports. Mexico eased its ban on U.S. poultry products on Monday, March 8, just two weeks after it was imposed when highly contagious bird flu was found in Texas. Mexico will allow imports of chicken pastes and deboned turkey and chicken from most U.S. states,** Javier Trujillo, the ministry's agricultural health chief, said. "The measure has been applied as of today," Trujillo said. Mexico is the fourth−largest importer of U.S. poultry, buying $93 million worth of chicken and related products in 2003. **The easing of the ban does not apply to 10 U.S. states where bird flu has been present for an extended period, Trujillo said.** Mexico closed its borders in 2002 to poultry imports from North Carolina, Maine, Pennsylvania, Virginia, West Virginia, Texas, California, and Connecticut due to bird flu. Imports from Delaware and New Jersey were banned later.
Source: http://www.reuters.com/newsArticle.jhtml?type=domesticNews&s

toryID=4520730&section=news

[Return to top]

Water Sector

16. *March 08, Associated Press* — **Water needs spur debate over growth. Las Vegas, NV, is turning to neighboring counties to the north to supply the nation's largest man−made reservoir. Plans include drilling wells and building a pipeline to tap rivers and groundwater from neighboring rural counties.** The Southern Nevada Water Authority says there is enough water out there to let the Las Vegas area population nearly double in the next decade without drawing more from the Colorado River that supplies Lake Mead. **Some at the head of the proposed pipeline worry that their high desert valleys and ranches will dry up if underground water is pumped to Las Vegas. They say the obvious solution is being ignored. "You have growth in an area that doesn't have water and the decisions aren't how to control growth, it's how to get water,"** said Paul Johnson, chairman of the White Pine County Commission in Ely, 250 miles north of Las Vegas. Johnson also sees parallels in the early 1900s Los Angeles water project that drained a valley north of Los Angeles and turned Owens Lake, east of the Sierra, into a dust bowl. Nevada in 2003 led the nation in population increase for a 17th year, according to the state demographer. About 80 percent of new residents moved to Las Vegas or nearby. The Lake Mead reservoir behind Hoover Dam is at its lowest level in 35 years, at 1,140 feet above sea level, or 65 feet below its high water mark. Source: http://www.sltrib.com/2004/Mar/03072004/utah/145502.asp

17. *March 07, Los Angeles Times* — **Pollution seeps near Los Angeles area's water source. Pacific Gas & Electric Co. is poised to begin pumping polluted groundwater from under the Mojave Desert to stop the toxic chemical hexavalent chromium from seeping into the Colorado River and tainting the water supply of 18 million Californians.** The chemical compound is ``on the brink of contaminating the Colorado River," the Metropolitan Water District of Southern California warned in a February 11 letter to state regulators. The toxic plume is emanating from land near PG&E's Topock natural−gas compressor station, south of Needles on California's border with Arizona. **The plume of at least 108 million gallons of chromium 6−tainted water is now threatening the river and causing alarm among experts at the Metropolitan Water District, which operates the Colorado River Aqueduct, a major source of Los Angeles' drinking water.** "The plume has moved past the last sentry well. It's thought to be 125 feet from the river, said Lisa Anderson, an environmental engineer at the water district's headquarters in Los Angeles. **The mass of the plume, just a few hundred feet behind the leading edge, measures more than 12,000 parts per bilion, and the maximum legal contaminant level for all types of chromium in drinking water is 50 parts per billion.** Source: http://www.mercurynews.com/mld/mercurynews/news/world/812818 0.htm

[Return to top]

Public Health Sector

18.

March 08, Washington University — **Device traps and deactivates airborne viruses and bacteria. An environmental engineer at Washington University in St. Louis with his doctoral student has patented a device for trapping and deactivating microbial particles. The work is promising in the war on terrorism for deactivating airborne bioagents and bioweapons, and also in routine indoor air ventilation applications such as in buildings and aircraft cabins.** Pratim Biswas, Professor of Environmental Engineering Sciences, combines an electrical field with soft X−rays and smart catalysts to capture and destroy bioagents such as the smallpox virus. **"When the aerosol particles come into the device they are charged and trapped in an electrical field," Biswas explained. "Any organic material is oxidized, so it completely deactivates the organism."** Biswas noted that conventional corona systems do not charge and effectively trap nanometer−sized particles, such as viruses. But his invention combines soft x−rays with a conventional corona that has been proven to be very effective at charging and trapping particles in a range of sizes.
Source: http://www.innovations−report.com/html/reports/life_sciences /report−26645.html

19. *March 07, Los Angeles Times* — **Science takes aim at terror.** The Bush administration has launched a vast research and development enterprise that will span many years. On the drawing boards is a far−reaching research project involving more than a dozen federal agencies that are managing work by thousands of scientists at hundreds of institutions and laboratories. At least seven billion dollars this year is slated for high−tech efforts to shore up defenses against a terrorist attack using biological, chemical, or nuclear weapons. Federal agencies are investing $3.5 billion in research and development and as much as $3.4 billion for vaccine supplies and improvements to the public health system. **Scientists see major population centers continuously monitored by remote detectors for evidence of a biological or chemical attack, and the nation's health care system equipped to handle mass epidemics spread by terrorists. Advanced research would deal with threats that don't even exist yet, such as biologically engineered diseases.**
Source: http://www.buffalonews.com/editorial/20040307/1053385.asp

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *March 09, The Age (Australia)* — **Bid to restrict fertilizer used in bombs.** The Australian Federal Government is set to toughen access to ammonium nitrate, the common fertilizer used by terrorists to make simple, but powerful bombs. **Andrew Metcalfe, deputy secretary of the Department of Prime Minister and Cabinet, told a parliamentary committee that ammonium nitrate headed the list of chemicals being examined in a nationwide review overseen by the Council of Australian Governments.** Metcalfe said ammonium nitrate was a serious concern because it had been used by terrorists, was easily obtainable and was widely used for blasting in the mining industry. He said the review was also looking at the availability

and use of a range of biological and radiological materials. An estimated 2200 kilograms of ammonium nitrate was used in the 1995 Oklahoma bombing that killed 168 people. Metcalfe said 900,000 tons of the chemical was used in Australia each year and the states and territories had been consulted extensively on ways to lessen the risks associated with it. "We had consultations with industry last week, with manufacturers, transporters and users and we expect that recommendations and advice will be going to government in the near future," he said. Metcalfe said the review had looked at ways to modify the fertilizer to make it less dangerous but that had been ruled out.
Source: http://www.theage.com.au/articles/2004/03/08/1078594297583.h tml

21. *March 09, Government Technology* — **New Jersey upgrades 911 technology.** New Jersey Gov. James E. McGreevey outlined the critical need of updating the state's 911 emergency response system recently at the State Police Operational Dispatch Center in Totowa. "911 was designed as a means of getting rapid response during emergency situations," said McGreevey. "With the current system in place, those who dial 911 from cell phones in remote areas throughout the state may not get the immediate attention needed in an emergency. The improved technology, funded through a cell tower assessment, will enable 911 dispatchers to locate a call made from a cell phone within 50 meters." The governor was joined by Albert J. Kernagis, state police deputy superintendent of operations, members of the New Jersey State Police and Jason Learn, a survivor of a 911 call who spent hours talking to a 911 dispatcher so rescue teams could locate him and his friends. **Scheduled to begin in late March, the upgrades will be the first of many steps necessary in deploying the technology necessary to locate 911 calls placed from cell phones. The network upgrade is expected to be completed this fall, at which time each of the six nationwide wireless carriers will begin to connect their location equipment to the statewide 911 networks.**
Source: http://www.govtech.net/news/news.php?id=89619

22. *March 08, The Mirror (UK)* — **Go ahead for first transatlantic emergency exercise.** Britain and America will stage a mock al Qaeda−style terrorist attack on both sides of the Atlantic to test security. **Home Secretary David Blunkett flew to Washington, DC, yesterday, March 7, to help plan the simultaneous exercise, set for next year. It will be the first joint operation of its kind and follows Britain's test of emergency services last September with a make−believe chemical attack on the London Underground. Blunkett says the idea is to highlight any gaps in anti−terrorist defenses or responses.** He explained yesterday that computer simulations could only provide part of the picture. "There are lots of desktop exercises going on all the time," he said. "But we need to set up a proper exercise so we can see what would happen in reality. We have to be prepared. And the way to do that is with a fully−fledged operational exercise." Likely scenarios include a 'dirty bomb' filled with radioactive material detonated during a city centre suicide attack. Other possibilities include a chemical or biological atrocity; an assault on a nuclear plant; a cyber attack that paralyses vital computer systems and causes economic havoc; a bomb attack on a motorway by either a vehicle or light plane.
Source: http://www.mirror.co.uk/news/allnews/content_objectid=14027053_method=full_siteid=50143_headline=−UK−AND−USA−IN−TERROR−TEST−II−name_page.html

23.

March 08, Federal Computer Week — **Homeland Security expands net to states, urban areas.** For the first time, federal, state and local agencies will be linked together by way of the Homeland Security Information Network (HSIN), launched late last month, which officials said represents an important step toward cooperation among the different levels of government. The network expands the Joint Regional Information Exchange System (JRIES), a network that government officials in New York and California have been developing with the Defense Intelligence Agency for the past several years. One of the biggest advantages to using that system as the starting point for HSIN is that state and local agencies that were testing JRIES were the ones to bring it to the Department of Homeland Security (DHS) and request that it be enhanced for national use, DHS Secretary Tom Ridge said at the launch February 24. **By the end of the year, DHS, all 50 states, five territories, Washington, DC, and 50 other major urban areas will be connected through the secure network, Ridge said. In the future, more cities, territories and other U.S. entities will be included — even the private sector, Ridge said.**
Source: http://www.fcw.com/fcw/articles/2004/0308/news−dhs−03−08−04. asp

[Return to top]

Information and Telecommunications Sector

24. *March 08, Techworld.com* — **HP fixes hole in Tru64.** HP Tru64 Unix, Hewlett−Packard Co.'s OS, has been found to suffer from "highly critical" security flaws involving remote access to systems. According to security site Secunia, HP has revealed little detail about what the vulnerabilities exactly are nor who they are most likely to affect, only that it has "fixed some vulnerabilities in Tru64, which potentially can be exploited by malicious people to compromise a vulnerable system" and that "**the vulnerabilities are caused due to unspecified errors within the certificate handling of IPsec/IKE."** Versions affected are 5.1B PK2(BL22) and PK3(BL24), and 5.1A PK6(BL24).
Source: http://www.computerworld.com.au/index.php?id=992016212&fp=16 &fpid=0

25. *March 08, eWEEK* — **Worm masquerades as Microsoft patch.** A new worm purporting to contain a patch to defend against MyDoom is attacking Windows machines throughout Europe and parts of North America. **Sober.D appeared Sunday, March 7, and began spreading in Germany and the United Kingdom. The worm arrives in an e−mail message with a subject line of "Microsoft Alert: Please Read!" and carries a sending address with a Microsoft domain**. The domain extension on the messages are typically from Germany, Israel, Switzerland or Austria. Many of the samples of the new variant that anti−virus vendors have seen so far have been written in German. The message includes a file attachment that is either an executable or a Zip archive, according to Network Associates Inc. Once installed on a machine, the virus will display a phony error message indicating either that the fake patch has been installed or does not need to be installed on the PC. Sober.D then scours the machine's hard drive for e−mail addresses and begins mailing itself out.
Source: http://www.eweek.com/article2/0,4149,1544482,00.asp?kc=EWRSS03119TX1K0000594

26. *March 04, eSecurity Planet* — **Buffer overflow detected in Adobe Reader.** Security researchers on Thursday, March 4, warned of a "high risk" buffer overflow flaw in some

versions of the Adobe Acrobat Reader that put users at risk of system takeover. British security consultants NGSSoftware detected the vulnerability in the XML forms data format (".xfdf") and warned that **a malicious attacker could cause a buffer overflow by tricking a user into viewing a specially crafted XFDF document**. The vulnerability affects Adobe Acrobat Reader 5.x. Adobe has corrected the flaw and is urging users to upgrade to the newer Adobe 6.0 software. According to the NGSSoftware advisory, the flaw is particularly serious because XFDF files with a ".xfdf" extension are rendered automatically on download when using applications like Microsoft's Internet Explorer browser.
Source: http://www.esecurityplanet.com/prodser/article.php/3321771

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_NETSKY.C** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	3127 (mydoom), 80 (www), 445 (microsoft−ds), 135 (epmap), 1434 (ms−sql−m), 4000 (Connect−BackBackdoor), 137 (netbios−ns), 4899 (radmin), 17300 (Kuang2TheVirus), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *March 08, Washington Post* — **Iraq council signs interim constitution.** Iraq's Governing Council signed a landmark interim constitution on Monday, March 8, that establishes a framework for democratic self−rule after the U.S. civil occupation ends this summer. The interim constitution calls for elections to be held by the end of January 2005 to select a 275−member transitional assembly. That group will serve as a legislature, draft a constitution and choose the president and two deputy presidents. The presidents, in turn, will select a prime minister and a cabinet to run the government. The transitional government will remain in power until a permanent constitution is approved in a national referendum and new elections are held. **The interim constitution includes a 13−article bill of rights that provides broad protections for individual liberties, guaranteeing freedom of speech, assembly, religion and other rights long denied by former president Saddam Hussein's Baath Party government**. The charter declares Islam to be "the official religion of the state," but only "a source" of legislation. In an apparent effort to placate conservative Shiites while providing

protections against religious domination, the document states that legislation cannot be enacted during the transition that infringes upon the "universally agreed upon tenets of Islam," but also that legislation cannot contradict any of the rights stipulated in the bill of rights.
Source: http://www.washingtonpost.com/wp−dyn/articles/A39476−2004Mar 8.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nicc@dhs.gov or call (202)323−3204.

DHS/IAIP Disclaimer